UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/580,689 | 05/30/2000 | Arturo Maria | 113639 | 1763 |

24197 7590 01/13/2005

KLARQUIST SPARKMAN, LLP
121 SW SALMON STREET
SUITE 1600
PORTLAND, OR 97204

| EXAMINER | |
|---|---|
| COLIN, CARL G | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2136 | |

DATE MAILED: 01/13/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/580,689 | MARIA, ARTURO | |
| | Examin r | Art Unit | |
| | Carl Colin | 2136 | |

*-- The MAILING DATE of this communication appears on the cover she t with the correspond nc address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *10/06/2004* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-5,7-30 and 32-38* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5,7-30 and 32-38* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 May 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

**Priority under 35 U.S.C. §§ 119 and 120**

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other:

## DETAILED ACTION

### *Response to Arguments*

1. In response to communications filed on 10/06/2004, Applicant cancels claims 6 and 31 and amends claims 1, 7, 15, 23, and 30. The following claims 1-5, 7-30, and 32-38 are presented for examination.

1.1 Applicant's arguments, pages 13-14, filed on 3/16/2004, with respect to the rejection of claims 1, 15, 23, and 30 have been fully considered but they are moot in view of a new ground of rejection.

### *Claim Objections*

2. Claim 32 is objected to because of the following informalities: claim 32 is dependent from claim 31, which is a cancelled claim. Appropriate correction is required.

### *Claim Rejections - 35 USC § 112*

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter, which the applicant regards as his invention.

Claims 15 and the intervening claims are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

3.1 Claim 15 recites the limitation "executing said intrusion detection software". There is insufficient antecedent basis for this limitation in the claim.

***Claim Rejections - 35 USC § 102***

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

4.1 **Claims 1-4, 6-11, 13-17, 19-25, 27-36, and 38** are rejected under 35 U.S.C. 102(e) as being anticipated by Non-Patent Literature by Raj Yavatkar, David Putzolu, Sanjay Bakshi, Satyendra Yadav, "The Phoenix Framework: A Practical Architecture for Programmable Networks"; March 2000; IEEE Communications Magazine; Pages 160-165.

4.2 **As per claims 1 and 30, Yavatkar et al** discloses a method for implementing an intrusion detection system in a network, comprising receiving a request at a software agent program to initiate intrusion detection services on a remote computer wherein the request is issued in response to a notification of a network intrusion, for example (see page 165, first column; see also page 163, second column); and discloses the launching of mobile agent which also can install code into the device that meets the recitation of installing intrusion detection software on said remote computer via said software agent program, for example (see page 165, first column); and executing said intrusion detection software on said remote computer via said software agent program, for example (see page 165, first column and conclusion); **Yavatkar et al** provides additional disclosure on page 161 about installing and executing intrusion detection software on a remote computer.

**As per claim 15, Yavatkar et al** discloses a method for implementing an intrusion detection system on a computer connected to a network, comprising receiving a request to become an intrusion detection platform from a remote network location, for example (see page 165, first column see also page 163, second column); wherein the request is issued in response to a notification of a network intrusion, for example (see page 165, first column see also page 163, second column); and executing said intrusion detection software, for example (see page 165, first column see also page 163, second column).

**As per claim 16, Yavatkar et al** discloses the limitation of installing intrusion detection software on said computer, for example (see page 165, first column see also page 163, second column).

**As per claim 23, Yavatkar et al** discloses a system for detecting intrusions in a computer network comprising: a plurality of computers executing software agents (page 162, column 2: configuration); an intrusion detection server (see figure 4) any network device can be acted as an instruction server without departing from the spirit and scope of the invention disclosed by **Yavatkar et al**; and a database configured to store at least one rule defining at least one response to a network intrusion, wherein said intrusion detection server sends a request to execute intrusion detection software to a software agent at least one of said plurality of computers when intrusion detection services are needed based on the at least one rule stored in said database (see page 162 and page 165, first column).

**As per claim 2, Yavatkar et al** discloses that third parties can request mobile agents to start, suspend, stop, and destroy services that meets the recitation of receiving a request to terminate intrusion detection services at said software agent program (see page 161, second column).

**As per claims 3 and 20, Yavatkar et al** discloses the limitation of monitoring for fulfillment of a stop condition (see congestion analysis, page 164 *with emphasis on second column, first paragraph )*.

**As per claims 4, 13, 19, and 38, Yavatkar et al** discloses the limitation of wherein said stop condition is based on network traffic conditions (see congestion analysis, page 164 *with emphasis on second column, first paragraph)*.

**As per claims 7 and 32, Yavatkar et al** discloses the limitation of selecting said remote computer from a plurality of eligible computers (see page 162 and page 165, first column).

**As per claims 8 and 33, Yavatkar et al** discloses the limitation of wherein said selecting step is accomplished based on a network physical topology of the network that meets the recitation of said selecting step is accomplished based on a network map (page 162 and page 165, first column).

**As per claims 9, 29, and 34, Yavatkar et al** discloses the limitation of wherein said selecting step is accomplished based on a knowledge base (page 162, second column, paragraphs 1 and 2).

**As per claims 10, 14, 21, and 35, Yavatkar et al** discloses security services for agent authentication authentication and authority that meets the limitation of wherein said request is verified using a cryptographic authentication scheme (page 161, column 2: proactive services).

**As per claims 11, 17, and 36, Yavatkar et al** discloses the limitation of wherein said request includes a stop condition indicating when to stop executing the intrusion detection software program, for example (see page 161, second column).

**As per claim 22, Yavatkar et al** discloses that third parties can request mobile agents to start, suspend, stop, and destroy services that meets the recitation of when said intrusion detection software has ceased executing, un-installing said intrusion detection software (see page 161, second column).

**As per claim 24, Yavatkar et al** discloses the limitation of wherein said intrusion detection server increases the number of said plurality of computers executing intrusion detection software when a network intrusion is detected (see page 162).

**As per claim 25, Yavatkar et al** discloses the limitation of wherein said intrusion detection server changes the number of said plurality of computers executing intrusion detection software when the level of network traffic changes (see page 162).

**As per claim 27, Yavatkar et al** discloses the limitation of wherein said database contains information about the plurality of computers (see page 162).

**As per claim 28, Yavatkar et al** discloses the limitation of wherein said information includes a map of said computer network (page 162 and page 165, first column).

***Claim Rejections - 35 USC § 103***

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5.1 **Claims 5, 12, 18, 26, and 37** are rejected under 35 U.S.C. 103(a) as being unpatentable over Raj Yavatkar, David Putzolu, Sanjay Bakshi, Satyendra Yadav, "The Phoenix Framework: A Practical Architecture for Programmable Networks"; March 2000; IEEE Communications Magazine; Pages 160-165, in view of US Patent 6,484,203 to **Porras et al**.

5.2 **As per claims 5, 12, 18, and 37, Yavatkar et al** substantially discloses monitoring stop condition with respect to network traffic, but does not explicitly disclose wherein said stop condition is an expiration time. **Porras et al** in an analogous art teaches an event monitoring and analysis including deploying network monitors wherein the client can request the server to terminate the monitoring because of slow response that meets the recitation of wherein the stop condition is an expiration time, for example (see column 9, lines 35-50). Therefore, it would

have been obvious to one of ordinary skill in the art at the time the invention was made to set a stop condition based on expiration time in order to manage a channel synchronization between the devices and monitor connection failure as taught by **Porras et al**. This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Porras et al** so as to provide continuous measures not only for intrusion detection but also to support the monitoring of the health and status of the network from the prospective of connectivity and throughput (column 5, lines 35-45).

**As per claim 26, Yavatkar et al** substantially discloses providing new network resources as required to take action to alleviate congestion (page 164). **Porras et al** refers to time of day when network traffic is heavier than other time of day (column 5, lines 22-45). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have the intrusion detection server changed the number of said plurality of computers executing intrusion detection software depending on the time of day as suggested by both references. This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Yavatkar et al** so as to implement the service in the most efficient manner (page 164, second column).

***Conclusion***

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

cc

Carl Colin

Patent Examiner

January 7, 2005

EMMANUEL L. MOISE
PRIMARY EXAMINER